

PEARSON WARSHAW, LLP  
15165 VENTURA BOULEVARD, SUITE 400  
SHERMAN OAKS, CALIFORNIA 91403

1 DANIEL L. WARSHAW (Bar No. 185365)

2 dwarshaw@pwfirm.com

3 **PEARSON WARSHAW, LLP**

4 15165 Ventura Boulevard, Suite 400

5 Sherman Oaks, California 91403

6 Telephone: (818) 788-8300

7 Facsimile: (818) 788-8104

8 STEVEN M. NATHAN, (Bar No. 153250)

9 snathan@hausfeld.com

10 **HAUSFELD LLP**

11 33 Whitehall Street

12 Fourteenth Floor

13 New York, NY 10004

14 Telephone: (646) 357-1100

15 Facsimile: (212) 202-4322

16 *Attorneys for Plaintiff and the Proposed*  
17 *Class*

18 **UNITED STATES DISTRICT COURT**

19 **CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION**

20 **BRUCE MARTIN**, individually and on  
21 behalf of all others similarly situated,

22 Plaintiff,

23 v.

24 **LOANDEPOT, INC.,**

25 Defendant.

CASE NO. 8:24-cv-265

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 Plaintiff Bruce Martin (“Plaintiff”), individually, and on behalf of all others  
2 similarly situated, brings this action against Defendant loanDepot, Inc. (“Defendant”  
3 or “loanDepot”). Plaintiff brings this action by and through his attorneys, and alleges,  
4 based upon personal knowledge as to his own actions, and based upon his information  
5 and belief and reasonable investigation by his counsel as to all other matters, as  
6 follows.

## 7 INTRODUCTION

8 1. This class action arises out of the recent targeted cyberattack and data  
9 breach on loanDepot’s network that resulted in unauthorized access to highly-  
10 sensitive data belonging to Plaintiff and approximately 16,600,000<sup>1</sup> Class Members  
11 (the “Data Breach”).

12 2. Defendant loanDepot is a California-based retail mortgage lender and  
13 nonbank holding company. Founded in 2010, loanDepot has “grown to become the  
14 nation’s fifth largest retail mortgage lender and the second largest nonbank retail  
15 originator, funding more than \$300 billion since inception. Today, [loanDepot’s]  
16 nationwide team of nearly 11,000 team members assists more than 30,000 customers  
17 each month.”<sup>2</sup>

18 3. As part of its business operations, loanDepot acquires, collects,  
19 maintains, and stores the highly-sensitive private information of its customers,  
20 including personally identifying information (“PII”) and sensitive financial  
21 information (collectively, “Private Information”).  
22  
23  
24

25 <sup>1</sup> loanDepot, *loanDepot provides Update on Cyber Incident*, Jan. 22, 2024,  
26 <https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx> (last visited Feb. 6, 2024); *see also*  
27 loanDepot, *loanDepot is experiencing a cyber incident*,  
28 <https://loandepot.cyberincidentupdate.com/> (last visited Feb. 6, 2024).

<sup>2</sup> loanDepot, *About Us*, <https://loandepot.com/about/> (last visited Feb. 6, 2024).

4. Defendant loanDepot claims it “believes in protecting the confidentiality and security of the information [it] collect[s] about [its] customer[s], potential customer[s], former customer[s], job applicant[s], [and] employee[s].”<sup>3</sup>

5. Despite these outward assurances, loanDepot failed to adequately safeguard Plaintiff’s and Class Members’ highly sensitive Private Information, which it collected and maintained.

6. On or about January 8, 2024, loanDepot reported it “recently identified a cybersecurity incident affecting certain of [loanDepot’s] systems.”<sup>4</sup>

7. According to loanDepot, the cyberattack targeted its phone and loan processing services, exposing sensitive Private Information belonging to 16.6 million consumers in its systems.<sup>5</sup>

8. As of the date of this filing, loanDepot still has not confirmed the specific type(s) of information compromised in the Data Breach.<sup>6</sup>

9. Upon information and belief, cybercriminals accessed and stole Private Information belonging to Plaintiff and Class Members, including, without limitation, their financial information, tax information, insurance information, credit history, employment data, driver’s licenses, and Social Security numbers.<sup>7</sup>

<sup>3</sup> loanDepot, *Privacy Policy*, <https://www.loandepot.com/privacypolicy> (last visited Feb. 5, 2024).

<sup>4</sup> United States Securities and Exchange Commission, *FORM 8-K -- loanDepot, Inc.* (Jan. 8, 2024), <https://www.sec.gov/Archives/edgar/data/1831631/000183163124000004/ldi-20240104.htm>.

<sup>5</sup> loanDepot, *loanDepot provides Update on Cyber Incident*, Jan. 22, 2024, <https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx>; *see also* loanDepot, *loanDepot is experiencing a cyber incident*, <https://loandepot.cyberincidentupdate.com/> (last visited Feb. 6, 2024).

<sup>6</sup> *See id.*; *see also* loanDepot, *loanDepot is experiencing a cyber incident*, <https://loandepot.cyberincidentupdate.com/> (last visited Feb. 6, 2024).

<sup>7</sup> *See* Kennedy Edgerton, *Mortgage Giant LoanDepot Now Says Cyberattack Exposed 16 Million Customers’ Personal Info*, *Forbes* (Jan. 24, 2024), <https://www.forbes.com/advisor/mortgages/loan-depot-mortgage-cyberattack->

10. Defendant loanDepot owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information. Yet, loanDepot maintained and shared the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on computer systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to loanDepot, and thus loanDepot was on notice that failing to take steps necessary to properly safeguard Plaintiff's and Class Members' Private Information from those risks left the Private Information in a vulnerable condition.

11. Ultimately, loanDepot failed to fulfill these obligations as unauthorized cybercriminals breached loanDepot's information systems and databases, and upon information and belief, stole vast quantities of Private Information belonging to Plaintiff and Class Members. This breach—and the compromise of Private Information—were direct, proximate, and foreseeable results of multiple failings by loanDepot.

12. Plaintiff's and Class Members' Private Information was compromised due to loanDepot's negligent and/or careless acts and omissions and loanDepot's failure to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

13. The Data Breach occurred because loanDepot inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. loanDepot also inexcusably failed to timely detect the Data Breach. And before the Data Breach occurred, loanDepot failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class Members been made aware of this fact, they would have never provided such information to \_\_\_\_\_  
update/.

1 loanDepot and/or loanDepot's business associates.

2 14. As a result of the Data Breach, Plaintiff and Class Members face a  
3 substantial risk of imminent and certainly impending harm, heightened by the loss of  
4 Social Security numbers, a class of Private Information which is particularly valuable  
5 to identity thieves. Plaintiff and Class Members have and will continue to suffer  
6 injuries associated with this risk, including but not limited to loss of time, mitigation  
7 expenses, and anxiety over misuse of their Private Information.

8 15. This risk is even more pronounced given the extended amount of time  
9 that lapsed between when the Data Breach occurred, when Defendant reportedly  
10 determined Plaintiff's and Class Members' Private Information was compromised,  
11 and when Defendant actually notified Plaintiff and Class Members about the Data  
12 Breach.

13 16. Even those Class Members who have yet to experience identity theft  
14 have to spend time responding to the Data Breach and are at an immediate and  
15 heightened risk of all manners of identity theft as a direct and proximate result of the  
16 Data Breach. Plaintiff and Class Members have incurred, and will continue to incur,  
17 damages in the form of, among other things, identity theft, attempted identity theft,  
18 lost time and expenses mitigating harms, increased risk of harm, damaged credit,  
19 diminished value of Private Information, loss of privacy, and/or additional damages  
20 as described below.

21 17. As a result of loanDepot's negligent, reckless, intentional, and/or  
22 unconscionable failure to adequately satisfy its contractual, statutory, and common-  
23 law obligations, Plaintiff and Class Members suffered injuries including, but not  
24 limited to:

- 25 • Lost or diminished value of their Private Information;
- 26 • Out-of-pocket expenses associated with the
- 27 prevention, detection, and recovery from identity theft,
- 28 tax fraud, and/or unauthorized use of their Private  
Information;

- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in loanDepot's possession and is subject to further unauthorized disclosures so long as loanDepot fails to undertake appropriate and adequate measures to protect their Private Information.

18. Accordingly, Plaintiff brings this action on behalf of all those similarly situated seeking relief for the consequences of loanDepot's failure to reasonably safeguard Plaintiff's and Class Members' Private Information; its failure to reasonably provide timely notification that Plaintiff's and Class Members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class Members concerning the status, safety, and protection of their Private Information.

19. Plaintiff brings this action against loanDepot, seeking redress for loanDepot's unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; (iv) bailment; and (v) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to loanDepot's data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by loanDepot.

### **PARTIES**

20. Plaintiff Bruce Martin is a resident and citizen of the State of Tennessee residing in Putnam County.

21. Defendant loanDepot, Inc. is a corporation organized under the laws of Delaware with its corporate headquarters and principal place of business located at 6561 Irvine Center Drive, Irvine, California 92618.

### **JURISDICTION AND VENUE**

22. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

23. This Court has general personal jurisdiction over Defendant because Defendant operates in and directs commerce at this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant has harmed Class Members residing in this District.

### **FACTUAL ALLEGATIONS**

#### **A. Defendant LoanDepot – Background**

25. Defendant loanDepot is a California-based retail mortgage lender and nonbank holding company, "assist[ing] more than 30,000 customers each month."<sup>8</sup>

26. On information and belief, in the ordinary course of its business, Defendant loanDepot maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number or taxpayer identification number;

<sup>8</sup> loanDepot, *About Us*, <https://loandepot.com/about/> (last visited Feb. 6, 2024).



- Financial and/or payment information; and
- Other information that Defendant loanDepot may deem necessary to provide services.

27. Additionally, Defendant loanDepot may receive Private Information from other individuals and/or organizations that are affiliated with the customer, such as their bank.

28. Because of the highly sensitive and personal nature of the information Defendant loanDepot acquires and stores with respect to consumers and other individuals, loanDepot, upon information and belief, promises to, among other things: keep Private Information private; comply with financial industry standards related to data security and Private Information, including FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from Defendant loanDepot and provide adequate notice to individuals if their Private Information is disclosed without authorization.

29. However, Defendant loanDepot did not maintain adequate security to protect its systems from infiltration by cybercriminals.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant loanDepot assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

31. Yet, contrary to Defendant's representations, loanDepot failed to implement adequate data security measures, as evidenced by Defendant's admission of the Data Breach, which affected approximately 16.6 million loanDepot current and former customers and employees.

32. Current and former customers of Defendant loanDepot, such as Plaintiff and Class Members, made their Private Information available to loanDepot with the



1 reasonable expectation that any entity with access to this information would keep that  
2 sensitive and personal information confidential and secure from illegal and  
3 unauthorized access. And, in the event of any unauthorized access, these entities  
4 would provide them with prompt and accurate notice.

5 33. This expectation was objectively reasonable and based on obligations  
6 imposed on loanDepot by statute, regulations, industry standards, and standards of  
7 general due care.

8 34. Unfortunately for Plaintiff and Class Members, loanDepot failed to carry  
9 out its duty to safeguard sensitive Private Information and provide adequate data  
10 security. As a result, loanDepot failed to protect Plaintiff and Class Members from  
11 having their Private Information accessed and stolen during the Data Breach.

#### 12 **B. The Data Breach and Notice Letter**

13 35. According to the notice posted on Defendant loanDepot's website (the  
14 "Data Breach Notice"),<sup>9</sup> loanDepot was subject to a cybersecurity attack that allowed  
15 unauthorized parties to access and compromise Plaintiff and Class Members' Private  
16 Information.

17 36. On or about January 8, 2024, loanDepot reported it "recently identified  
18 a cybersecurity incident affecting certain of [loanDepot's] systems."<sup>10</sup>

19 37. Upon detecting the unauthorized activity, loanDepot claims it "retained  
20 leading forensics experts to aid in [its] investigation[.]"<sup>11</sup>

21  
22  
23  
24  
25 <sup>9</sup> See loanDepot, *loanDepot provides Update on Cyber Incident*, Jan. 22, 2024,  
26 <https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx>; see also loanDepot, *loanDepot is experiencing a cyber incident*, <https://loandepot.cyberincidentupdate.com/> (last  
27 accessed Feb. 6, 2024); Data Breach Notice, **Exhibit A**.

28 <sup>10</sup> See *id.*

<sup>11</sup> *Id.*

1 38. According to loanDepot, the cyberattack targeted its phone and loan  
2 processing services, exposing sensitive Private Information belonging to 16.6 million  
3 consumers in its systems.<sup>12</sup>

4 39. As of the date of this filing, loanDepot still has not confirmed the specific  
5 type(s) of information compromised in the Data Breach.<sup>13</sup>

6 40. Upon information and belief, cybercriminals accessed and stole Private  
7 Information belonging to Plaintiff and Class Members, including, without limitation,  
8 their financial information, tax information, insurance information, credit history,  
9 employment data, driver's licenses, and Social Security numbers.<sup>14</sup>

10 41. In the aftermath of the Data Breach, Defendant loanDepot has not  
11 indicated what measures, if any, it has taken to mitigate the harm beyond "tak[ing]  
12 certain systems offline and [] working diligently to restore normal business operations  
13 as quickly as possible."<sup>15</sup> There is no indication whether these measures are adequate  
14 to protect Plaintiff's and Class Members' Private Information going forward.

15 42. According to Defendant loanDepot, Plaintiff's and Class Members'  
16 Private Information was exfiltrated and stolen in the Data Breach.

17 43. The accessed data contained Private Information that was accessible,  
18 unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the  
19 unauthorized actor.

20 44. As a highly sophisticated financial services business entity that collects,  
21 creates, and maintains significant volumes of Private Information, the targeted attack  
22 was a foreseeable risk which loanDepot was aware of and knew it had a duty to guard  
23

24 <sup>12</sup> See *id.*

25 <sup>13</sup> See *id.*

26 <sup>14</sup> See Kennedy Edgerton, *Mortgage Giant LoanDepot Now Says Cyberattack*  
27 *Exposed 16 Million Customers' Personal Info*, Forbes (Jan. 24, 2024),  
28 [https://www.forbes.com/advisor/mortgages/loan-depot-mortgage-cyberattack-](https://www.forbes.com/advisor/mortgages/loan-depot-mortgage-cyberattack-update/)  
update/.

<sup>15</sup> See Data Breach Notice, **Exhibit A**.

1 against. It is well-known that sophisticated business entities and their business  
2 associates such as Defendant, which collect and store the confidential and sensitive  
3 Private Information of millions of individuals, are frequently targeted by  
4 cyberattacks. Further, cyberattacks are highly preventable through the  
5 implementation of reasonable and adequate cybersecurity safeguards, including  
6 proper employee cybersecurity training.

7 45. The targeted cyberattack was expressly designed to gain access to and  
8 exfiltrate private and confidential data, including (among other things) the Private  
9 Information of consumers, like Plaintiff and Class Members.

10 46. Defendant had obligations created by contract, industry standards,  
11 common law, and its own promises and representations made to Plaintiff and Class  
12 Members to keep their Private Information confidential and protected from  
13 unauthorized access and disclosure.

14 47. Plaintiff and Class Members entrusted loanDepot with their Private  
15 Information with the reasonable expectation and mutual understanding that  
16 loanDepot would comply with its obligations to keep such information confidential  
17 and secure from unauthorized access.

18 48. By obtaining, collecting, using, and deriving a benefit from Plaintiff's  
19 and Class Members' Private Information, Defendant assumed legal and equitable  
20 duties and knew, or should have known, that it was responsible for protecting  
21 Plaintiff's and Class Members' Private Information from unauthorized disclosure.

22 49. Due to loanDepot's inadequate security measures and its delayed notice  
23 to victims, Plaintiff and Class Members now face a present, immediate, and ongoing  
24 risk of fraud and identity theft that they will have to deal with for the rest of their lives.

25 **C. Defendant's Failure to Protect Consumers' Private**  
26 **Information**

27 50. Defendant loanDepot collects and maintains vast quantities of Private  
28 Information as part of its normal operations as a financial services provider. The Data

1 Breach occurred as a direct, proximate, and foreseeable result of multiple failings on  
2 the part of loanDepot.

3 51. Defendant loanDepot inexcusably failed to implement reasonable  
4 security protections to safeguard its information systems and databases.

5 52. Defendant loanDepot failed to inform the public that its data security  
6 practices were deficient and inadequate. Had Plaintiff and Class Members been aware  
7 that loanDepot did not have adequate safeguards in place to protect their sensitive  
8 Private Information, they would have never provided such information to loanDepot.

9 53. Plaintiff's and Class Members' Private Information was accessed and  
10 acquired by cybercriminals for the express purpose of misusing the data. They face  
11 the real, immediate, and likely danger of identity theft and misuse of their Private  
12 Information. And this can, and in some circumstances already has, caused irreparable  
13 harm to their personal, financial, reputational, and future well-being.

14 **D. The Data Breach was a Foreseeable Risk of which Defendant**  
15 **was on Notice**

16 54. Data breaches have become a constant threat that, without adequate  
17 safeguards, can expose personal data to malicious actors. It is well known that PII,  
18 and Social Security numbers in particular, are an invaluable commodity and a frequent  
19 target of hackers.

20 55. As a sophisticated business entity handling confidential customer data,  
21 loanDepot's data security obligations were particularly important given the  
22 substantial increase in cyberattacks and/or data breaches in industries holding  
23 significant amounts of Private Information preceding the date of the Data Breach.

24 56. At all relevant times, Defendant knew, or should have known that  
25 Plaintiff's and Class Members' Private Information was a target for malicious actors.  
26 Despite such knowledge, loanDepot failed to implement and maintain reasonable and  
27 appropriate data privacy and security measures to protect Plaintiff's and Class  
28 Members' Private Information from cyberattacks that loanDepot should have

1 anticipated and guarded against.

2 57. In light of recent high profile data breaches at other financial services  
3 providers, Defendant knew or should have known that its electronic records and  
4 consumers' Private Information would be targeted by cybercriminals and  
5 ransomware attack groups.

6 58. Cyberattacks and data breaches of financial services companies are  
7 especially problematic because of the potentially permanent disruption they cause to  
8 the daily lives of their customers. Stories of identity theft and fraud abound, with  
9 hundreds of millions of dollars lost by everyday consumers every year as a result of  
10 internet-based identity theft attacks.<sup>16</sup>

11 59. The U.S. Government Accountability Office ("GAO") released a report  
12 on data breaches in 2007 (the "GAO Report"), finding that victims of identity theft  
13 will face "substantial costs and time to repair the damage to their good name and  
14 credit record."<sup>17</sup>

15 60. The FTC recommends that identity theft victims take several steps to  
16 protect their personal and financial information after a data breach, including  
17 contacting one of the credit bureaus to place a fraud alert (and to consider an extended  
18 fraud alert that lasts for seven years if identity theft occurs), reviewing their credit  
19 reports, contacting companies to remove fraudulent charges from their accounts,  
20 placing a credit freeze on their credit, and correcting their credit reports.<sup>18</sup>

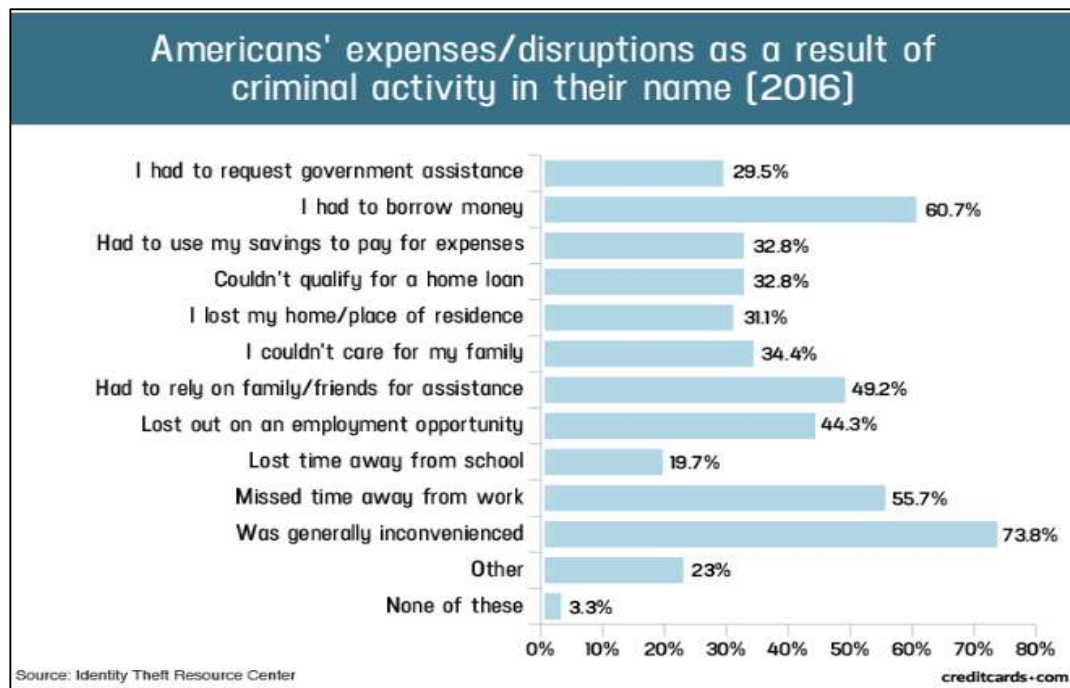
21  
22  
23 <sup>16</sup> Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most*  
24 *targeted)* (July 27, 2022), <https://www.komando.com/security-privacy/most-costly-data-breaches/847800/>

25 <sup>17</sup> See U.S. Gov. Accounting Office, *Personal Information: Data Breaches Are*  
26 *Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full*  
27 *Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007),  
<https://www.gao.gov/assets/270/262899.pdf> [<https://perma.cc/GCA5-WYA5>].

28 <sup>18</sup> *Identity Theft Recovery Steps*, FTC, <https://www.identitytheft.gov/Steps> (last visited Dec. 12, 2023) [<https://perma.cc/ME45-5N3A>].

61. Cybercriminals use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

62. Identity thieves can also use Social Security numbers to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's PII to police during an arrest, resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:<sup>19</sup>



<sup>19</sup> Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (updated Oct. 24, 2017), <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> [<https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>].



**E. Defendant Had a Duty and Obligation to Protect Private Information**

63. As set forth above, 96.7 percent of study subjects experienced costs or other harms as a result of criminal activity in their name.<sup>20</sup> As illustrated in the above graphic, this includes devastating results such as “I lost my home/place of residence” and “I couldn’t care for my family.” Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.<sup>21</sup> The ITRC study concludes that “identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual.”<sup>22</sup>

64. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of “phishing,” “vishing,” “smishing,” and “pharming,” which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

65. Notably, there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and between when PII and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*



1 used to commit identity theft. Further, once stolen data have  
2 been sold or posted on the Web, fraudulent use of that  
3 information may continue for years. As a result, studies that  
4 attempt to measure the harm resulting from data breaches  
cannot necessarily rule out all future harm.<sup>23</sup>

5 66. PII is such an inherently valuable commodity to identity thieves that,  
6 once compromised, criminals often trade the information on the dark web for years.

7 67. Furthermore, data breaches that expose personal data, and in particular  
8 non-public data of any kind directly and materially increase the chance that a potential  
9 victim will be targeted by a spear phishing attack in the future, and spear phishing  
10 results in a high rate of identity theft, fraud, and extortion.<sup>24</sup>

11 68. There is a strong probability that entire batches of stolen information  
12 from the Data Breach have yet to be made available on the black market, meaning  
13 Plaintiff and Class Members will remain at an increased risk of fraud and identity  
14 theft for many years into the future. Thus, as the loanDepot Data Breach Notice  
15 advises, Plaintiff must vigilantly monitor his financial accounts for many years to  
16 come.

17 69. As a highly sophisticated party that handles sensitive Private  
18 Information, Defendant failed to establish and/or implement appropriate  
19 administrative, technical and/or physical safeguards to ensure the security and  
20 confidentiality of Plaintiff's and Class Members' Private Information.

21 ///

22  
23 <sup>23</sup> GAO Report, *supra* n.17 **Error! Bookmark not defined.**, at 29.

24 <sup>24</sup> See Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*,  
25 BBC News (July 30, 2020), <https://www.bbc.com/news/technology-53567699>  
26 (concluding that personal information such as “names, titles, telephone numbers,  
27 email addresses, mailing addresses, dates of birth ... in the hands of fraudsters,  
28 [makes consumers] particularly susceptible to spear phishing—a fraudulent email to  
specific targets while purporting to be a trusted sender, with the aim of convincing  
victims to hand over information or money or infecting devices with malware”).

70. The ramifications of Defendant’s failure to keep Plaintiff’s and Class Members’ Private Information secure are severe and long-lasting. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the “dark web” may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts, and Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

71. Private Information, like that stolen from loanDepot, is “often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail.” The record sets are then sold on dark web sites to other criminals and “allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities.”<sup>25</sup>

72. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ Private Information has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

73. Statista, a German entity that collects and markets data relating to data breach incidents and their consequences, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005; it reported 157 compromises in 2005, to a peak of 1,862 in 2021, to 2022’s total of 1,802.<sup>26</sup> The number of impacted individuals has also risen precipitously from

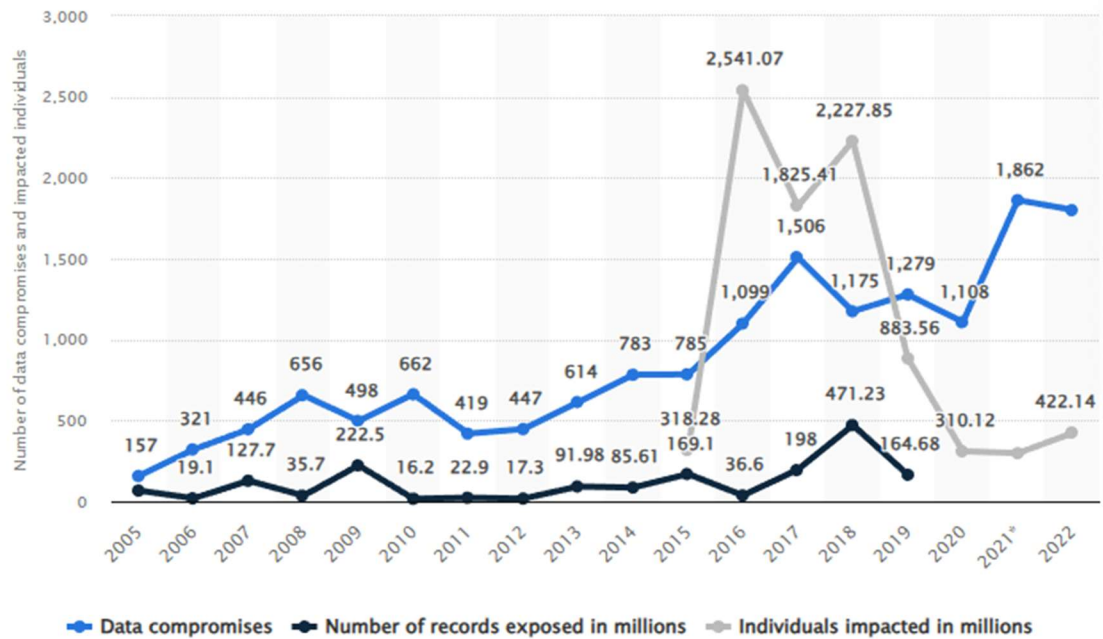
---

<sup>25</sup> See *id.*

<sup>26</sup> *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/> (last accessed Dec. 7, 2023).

1 approximately 318 million in 2015 to 422 million in 2022, which is an increase of  
2 nearly 50%.<sup>27</sup>

3 74. This stolen Private Information is then routinely traded on dark web  
4 black markets as a simple commodity.<sup>28</sup>



16 75. Armed with just a name and Social Security Number, criminals can  
17 fraudulently take out loans under a victims' name, open new lines of credit, and cause  
18 other serious financial difficulties for victims:

19 A dishonest person who has your Social Security number can  
20 use it to get other personal information about you. Identity  
21 thieves can use your number and your good credit to apply  
22 for more credit in your name. Then, they use the credit cards  
23 and don't pay the bills, it damages your credit. You may not  
24 find out that someone is using your number until you're  
25 turned down for credit, or you begin to get calls from  
26 unknown creditors demanding payment for items you never

27 *Id.*

28 <sup>28</sup> Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (Nov. 15, 2023), available at <https://cybernews.com/security/whats-your-identity-worth-on-dark-web/> (last accessed Dec. 7, 2023).

1 bought. Someone illegally using your Social Security  
2 number and a identity can cause a lot of problems.<sup>29</sup>

3 76. The problems associated with a compromised Social Security Number  
4 are exceedingly difficult to resolve. A victim is forbidden from proactively changing  
5 his or her number unless and until it is actually misused, and harm has already  
6 occurred. And even this delayed remedial action is unlikely to undo the damage  
7 already done to the victims:

8 Keep in mind that a new number probably won't solve all  
9 your problems. This is because other governmental  
10 agencies (such as the IRS and state motor vehicle agencies)  
11 and private businesses (such as banks and credit reporting  
12 companies) will have records under your old number.  
13 Along with other personal information, credit reporting  
14 companies use the number to identify your credit record. So  
15 using a new number won't guarantee you a fresh start. This  
16 is especially true if your other personal information, such as  
17 your name and address, remains the same.<sup>30</sup>

18 77. In addition, the Federal Trade Commission ("FTC") has brought dozens  
19 of cases against companies that have engaged in unfair or deceptive practices  
20 involving inadequate protection of consumers' personal data. The FTC publicized  
21 these enforcement actions to place companies like loanDepot on notice of their  
22 obligation to safeguard consumer information.

23 78. Thus, loanDepot knew, or should have known, the importance of  
24 safeguarding the Private Information entrusted to it and of the foreseeable  
25 consequences if its systems were breached. Defendant failed, however, to take  
26 adequate cybersecurity measures to prevent the Data Breach from occurring.

27 <sup>29</sup> United States Social Security Administration, *Identity Theft and Your Social*  
28 *Security Number*, United States Social Security Administration at 1 (July 2021),  
available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Dec. 7,  
2023).

<sup>30</sup> *Id.*

79. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, loanDepot failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by loanDepot's failure to implement or maintain adequate data security measures for its current and former customers.

#### **F. Defendant Had a Duty and Obligation to Protect Private Information**

80. Defendant loanDepot has an obligation to protect the Private Information belonging to Plaintiff and Class Members. First, this obligation was mandated by government regulations and state laws, including FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII. And third, loanDepot imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class Members provided, and loanDepot obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

##### **1. FTC Act Requirements and Violations**

81. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

82. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.<sup>31</sup> The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.<sup>32</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>33</sup> Defendant loanDepot clearly failed to do any of the foregoing, as evidenced by the Data Breach itself.

83. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

84. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

<sup>31</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last accessed Dec. 7, 2023).

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*



1           85. As evidenced by the Data Breach, loanDepot failed to properly  
2 implement basic data security practices. Defendant's failure to employ reasonable and  
3 appropriate measures to protect against unauthorized access to Plaintiff's and Class  
4 Members' Private Information constitutes an unfair act or practice prohibited by  
5 Section 5 of the FTC Act.

6           86. Defendant was fully aware of its obligation to protect the Private  
7 Information of its current and former customers, including Plaintiff and Class  
8 Members, as loanDepot is a sophisticated and technologically savvy financial services  
9 entity that relies extensively on technology systems and networks to maintain its  
10 practice, including storing its customers' PII and sensitive financial information in  
11 order to operate its business.

12           87. Defendant had and continues to have a duty to exercise reasonable care  
13 in collecting, storing, and protecting the Private Information of Plaintiff and the Class  
14 from the foreseeable risk of a data breach. The duty arises out of the special  
15 relationship that exists between loanDepot and Plaintiff and Class Members.  
16 Defendant alone had the exclusive ability to implement adequate security measures  
17 to its cyber security network to secure and protect Plaintiff's and Class Members'  
18 Private Information.

## 19                   2. Industry Standards and Noncompliance

20           88. As noted above, experts studying cybersecurity routinely identify  
21 businesses as being particularly vulnerable to cyberattacks because of the value of the  
22 Private Information that they collect and maintain.

23           89. Some industry best practices that should be implemented by businesses  
24 dealing with sensitive Private Information like loanDepot include, but are not limited  
25 to: educating all employees, strong password requirements, multilayer security  
26 including firewalls, anti-virus and anti-malware software, encryption, multi-factor  
27 authentication, backing up data, and limiting which employees can access sensitive  
28 data.



90. Other best cybersecurity practices that are standard in the financial services industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

91. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and loanDepot failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

### **G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft**

93. Cyberattacks and data breaches at financial service providers like Defendant loanDepot are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

94. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."<sup>34</sup>

<sup>34</sup> See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data*

95. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

96. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>35</sup>

97. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

///

*Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007),  
<https://www.gao.gov/new.items/d07737.pdf>.

<sup>35</sup> See *IdentityTheft.gov*, FEDERAL TRADE COMMISSION,  
<https://www.identitytheft.gov/Steps> (last visited Dec. 11, 2023).

1           98. Identity thieves can also use Social Security numbers to obtain a driver's  
2 license or official identification card in the victim's name but with the thief's picture;  
3 use the victim's name and Social Security number to obtain government benefits; or  
4 file a fraudulent tax return using the victim's information. In addition, identity thieves  
5 may obtain a job using the victim's Social Security number, rent a house or receive  
6 medical services in the victim's name, and may even give the victim's personal  
7 information to police during an arrest resulting in an arrest warrant being issued in  
8 the victim's name.

9           99. Moreover, theft of Private Information is also gravely serious because  
10 Private Information is an extremely valuable property right.<sup>36</sup>

11           100. Its value is axiomatic, considering the value of "big data" in corporate  
12 America and the fact that the consequences of cyber thefts include heavy prison  
13 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that  
14 Private Information has considerable market value.

15           101. It must also be noted there may be a substantial time lag – measured in  
16 years – between when harm occurs and when it is discovered, and also between when  
17 Private Information and/or financial information is stolen and when it is used.

18           102. According to the U.S. Government Accountability Office, which  
19 conducted a study regarding data breaches:

20                   [L]aw enforcement officials told us that in some cases,  
21 stolen data may be held for up to a year or more before being  
22 used to commit identity theft. Further, once stolen data have  
23 been sold or posted on the Web, fraudulent use of that  
24 information may continue for years. As a result, studies that  
attempt to measure the harm resulting from data breaches  
cannot necessarily rule out all future harm.

25  
26 <sup>36</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of*  
27 *Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*,  
28 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) ("PII, which companies obtain at little cost,  
has quantifiable value that is rapidly reaching a level comparable to the value of  
traditional financial assets.") (citations omitted).

1 GAO Report at 29.

2 103. Private Information is such a valuable commodity to identity thieves that  
3 once the information has been compromised, criminals often trade the information on  
4 the “cyber black-market” for years.

5 104. Thus, Plaintiff and Class Members must vigilantly monitor their  
6 financial accounts, or the accounts of deceased individuals for whom Class Members  
7 are the executors or surviving spouses, for many years to come.

8 105. Private Information is particularly valuable because criminals can use it  
9 to target victims with frauds and scams. Once Private Information is stolen, fraudulent  
10 use of that information and damage to victims may continue for years.

11 106. For example, the Social Security Administration has warned that identity  
12 thieves can use an individual’s Social Security number to apply for additional credit  
13 lines.<sup>37</sup> Such fraud may go undetected until debt collection calls commence months,  
14 or even years, later. Stolen Social Security numbers also make it possible for thieves  
15 to file fraudulent tax returns, file for unemployment benefits, or apply for a job using  
16 a false identity.<sup>38</sup> Each of these fraudulent activities is difficult to detect. An  
17 individual may not know that his or her Social Security number was used to file for  
18 unemployment benefits until law enforcement notifies the individual’s employer of  
19 the suspected fraud. Fraudulent tax returns are typically discovered only when an  
20 individual’s authentic tax return is rejected.

21 107. Moreover, it is not an easy task to change or cancel a stolen Social  
22 Security number.

23 108. An individual cannot obtain a new Social Security number without  
24 significant paperwork and evidence of actual misuse. Even then, a new Social  
25 Security number may not be effective, as “[t]he credit bureaus and banks are able to  
26

27 <sup>37</sup> *Identity Theft and Your Social Security Number*, Social Security Administration  
(July 2021), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

28 <sup>38</sup> *Id.*

1 link the new number very quickly to the old number, so all of that old bad information  
2 is quickly inherited into the new Social Security number.”<sup>39</sup>

3 109. This data, as one would expect, demands a much higher price on the  
4 black market. Martin Walter, senior director at the cybersecurity firm RedSeal,  
5 explained, “[c]ompared to credit card information, personally identifiable  
6 information and Social Security Numbers are worth more than 10x on the black  
7 market.”<sup>40</sup>

8 110. Because of the value of its collected and stored data, the financial  
9 services industry has experienced disproportionately higher numbers of data theft  
10 events than other industries.

11 111. For the foregoing reasons, Defendant loanDepot knew or should have  
12 known about these dangers and strengthened its data and email handling systems  
13 accordingly. Defendant loanDepot was on notice of the substantial and foreseeable  
14 risk of harm from a data breach, yet loanDepot failed to properly prepare for that risk.

#### 15 **H. Defendant loanDepot’s Data Breach**

16 112. Defendant loanDepot breached its obligations to Plaintiff and Class  
17 Members and/or was otherwise negligent and reckless because it failed to properly  
18 maintain and safeguard its computer systems and data. Defendant’s unlawful conduct  
19 includes, but is not limited to, the following acts and/or omissions:

- 20 a. Failing to maintain an adequate data security system
- 21 to reduce the risk of data breaches and cyber-attacks;
- 22 b. Failing to adequately protect consumers’ Private
- 23 Information;

24 <sup>39</sup> Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce*  
25 *Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

26 <sup>40</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*  
27 *Credit Card Numbers*, Computer World (Feb. 6, 2015),  
28 <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- g. Failing to adhere to industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

113. Defendant loanDepot negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

114. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

### **I. Plaintiff and the Class Suffered Harm Resulting from the Data Breach**

115. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendant has done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Defendant has not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of

1 the Data Breach.

2 116. The FTC warns the public to pay particular attention to how they keep  
3 PII, including Social Security numbers and other sensitive data. As the FTC notes,  
4 “once identity thieves have your personal information, they can drain your bank  
5 account, run up charges on your credit cards, open new utility accounts, or get medical  
6 treatment on your health insurance.”<sup>41</sup>

7 117. The ramifications of loanDepot’s failure to properly secure Plaintiff’s  
8 and Class Members’ Private Information are severe. Identity theft occurs when  
9 someone uses another person’s financial, medical, or personal information, such as  
10 that person’s name, address, Social Security number, and other information, without  
11 permission in order to commit fraud or other crimes.

12 118. PII has a long shelf-life because it can be used in more ways than one,  
13 and it typically takes time for an information breach to be detected.

14 119. Plaintiff and Class Members face an imminent and substantial risk of  
15 injury of identity theft and related cyber crimes due to the Data Breach. Once data  
16 is stolen, malicious actors will either exploit the data for profit themselves or sell  
17 the data on the dark web to someone who intends to exploit the data for profit.  
18 Hackers would not incur the time and effort to steal PII and then risk prosecution by  
19 listing it for sale on the dark web if the PII was not valuable to malicious actors.

20 120. The dark web helps ensure users’ privacy by effectively hiding server  
21 or IP details from the public. Users need special software to access the dark web.  
22 Most websites on the dark web are not directly accessible via traditional searches  
23 on common search engines and are therefore accessible only by users who know the  
24 addresses for those websites.

25  
26 \_\_\_\_\_  
27 <sup>41</sup> *Warning Signs of Identity Theft*, Federal Trade Comm’n, available at  
28 <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed Dec.  
7, 2023).



1 121. Malicious actors use Private Information to gain access to Class  
2 Members' digital life, including bank accounts, social media, and credit card details.  
3 During that process, hackers can harvest other sensitive data from the victim's  
4 accounts, including personal information of family, friends, and colleagues.

5 122. Consumers are injured every time their data is stolen and placed on the  
6 dark web, even if they have been victims of previous data breaches. Not only is the  
7 likelihood of identity theft increased, but the dark web is not like Google or eBay. It  
8 is comprised of multiple discrete repositories of stolen information. Each data breach  
9 puts victims at risk of having their information uploaded to different dark web  
10 databases and viewed and used by different criminal actors.

11 123. Malicious actors can use Class Members' Private Information to open  
12 new financial accounts, open new utility accounts, file fraudulent tax returns, obtain  
13 government benefits, obtain government IDs, or create "synthetic identities."

14 124. As established above, the Private Information accessed in the Data  
15 Breach is also very valuable to loanDepot. Defendant collects, retains, and uses this  
16 information to increase profits. Defendant's customers value the privacy of this  
17 information and expect loanDepot to allocate enough resources to ensure it is  
18 adequately protected. Customers would not have done business with loanDepot,  
19 provided their Private Information, and/or paid the same prices for loanDepot's  
20 services had they known loanDepot did not implement reasonable security measures  
21 to protect their Private Information. Consumers expect that the payments they make  
22 to financial services providers incorporate the costs to implement reasonable  
23 security measures to protect their Private Information.

24 125. The Private Information accessed in the Data Breach is also very  
25 valuable to Plaintiff and Class Members. Consumers often exchange personal  
26 information for goods and services. For example, consumers often exchange their  
27 personal information for access to Wi-Fi in places like airports and coffee shops.  
28 Likewise, consumers often trade their names and email addresses for special

1 discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use  
2 their unique and valuable PII to access the financial sector, including when obtaining  
3 a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff  
4 and Class Members' PII has been compromised and lost significant value.

5 126. Even when reimbursed for money stolen due to a data breach, consumers  
6 are not made whole because the reimbursement fails to compensate for the significant  
7 time and money required to repair the impact of the fraud.

8 127. Accordingly, loanDepot's wrongful actions and inaction and the  
9 resulting Data Breach have also placed Plaintiff and the Class at an imminent,  
10 immediate, and continuing increased risk of identity theft and identity fraud.

11 128. There is also a high likelihood that significant identity fraud and identity  
12 theft has not yet been discovered or reported. Even data that has not yet been exploited  
13 by cybercriminals may be exploited in the future; there is a concrete risk that the  
14 cybercriminals who now possess Class Members' Private Information will do so at a  
15 later date or re-sell it.

16 129. Data breaches have also proven to be costly for affected organizations as  
17 well, with the average cost to resolve a data breach in 2023 at \$4.45 million.<sup>42</sup>

18 130. Here, due to the Breach, Plaintiff and Class Members have been exposed  
19 to injuries that include, but are not limited to:

- 20 a. Theft of Private Information;
- 21 b. Costs associated with the detection and prevention of
- 22 identity theft and unauthorized use of financial
- 23 accounts as a direct and proximate result of the Private
- 24 Information stolen during the Data Breach;

25 <sup>42</sup> *Cost of a Data Breach Report 2023*, IBM Security, available at  
26 [https://www.ibm.com/reports/data-breach?utm\\_content=SRCWW&p1=Search&p4=](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclid=aw.ds)  
27 [43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclid=aw.ds)  
28 [0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD\\_BwE&gc](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclid=aw.ds)  
[lsrc=aw.ds](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclid=aw.ds) (last accessed Dec. 7, 2023).

- c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;
- d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; and
- e. The loss of Plaintiff's and Class Members' privacy.

131. Plaintiff and Class Members have suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will continue for years and years. The unauthorized access of Plaintiff's and Class Members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely.

132. As a direct and proximate result of loanDepot's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class Members have been placed at a substantial risk of harm in the form of identity theft and have incurred and will incur actual damages in an attempt to prevent identity theft.

133. In addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose Private Information was accessed in the Data Breach, Plaintiff retains an interest in ensuring there are no future breaches. On information and belief, loanDepot is still in possession, custody, or control of Plaintiff's and the Class Members' Private Information.

**J. Experiences Specific to Plaintiff**

134. Plaintiff Bruce Martin is a current customer of loanDepot.

135. According to the Data Breach Notice posted on loanDepot's website, Plaintiff's Private Information was impacted in the Data Breach.

136. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving services from loanDepot that required his Private Information. Upon information and belief, loanDepot received, stores, and maintains the Private Information Plaintiff was required to provide to receive services from loanDepot.

137. Plaintiff is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

138. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring his credit.

139. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

140. Plaintiff suffered actual injury and damages from having his Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time; (e) imminent and

1 impending injury arising from the increased risk of identity theft and fraud; (f) failure  
2 to receive the benefit of his bargain; and (g) nominal and statutory damages.

3 141. Plaintiff recently drove from Southern California to his new home in  
4 Tennessee to close on his new mortgage loan, serviced by loanDepot. As a result of  
5 the Data Breach, the closure was delayed for more than a week, leaving Plaintiff and  
6 his wife without a place to stay. Both suffered significant psychological distress from  
7 the incident.

8 142. Plaintiff has suffered emotional distress that is proportional to the risk of  
9 harm and loss of privacy caused by the theft of his Private Information, which he  
10 believed would be protected from unauthorized access and disclosure, including  
11 anxiety about unauthorized parties viewing, selling, and/or using his Private  
12 Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety  
13 about unauthorized parties viewing, using, and/or publishing information related to  
14 his Social Security number.

15 143. As a result of the Data Breach, Plaintiff anticipates spending  
16 considerable time and money on an ongoing basis to try to mitigate and address harms  
17 caused by the Data Breach. In addition, Plaintiff will continue to be at a present,  
18 imminent, and continued increased risk of identity theft and fraud in perpetuity.

19 144. Plaintiff has a continuing interest in ensuring that his Private  
20 Information, which, upon information and belief, remains backed up in Defendant's  
21 possession, is protected and safeguarded from future breaches.

### 22 CLASS REPRESENTATION ALLEGATIONS

23 145. Plaintiff brings this action against Defendant loanDepot individually and  
24 on behalf of all other persons similarly situated (the "Class").

25 146. Plaintiff proposes the following Class definition, subject to amendment  
26 as appropriate:

27 **All persons or, if minors, their parents or guardians, or,**  
28 **if deceased, their executors or surviving spouses, who**

**Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

147. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

148. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

149. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Approximately 16.6 million individuals were impacted by Defendant's Data Breach.<sup>43</sup>

150. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

///

<sup>43</sup> See Kennedy Edgerton, *Mortgage Giant LoanDepot Now Says Cyberattack Exposed 16 Million Customers' Personal Info*, Forbes (Jan. 24, 2024), <https://www.forbes.com/advisor/mortgages/loan-depot-mortgage-cyberattack-update/>.

- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Plaintiff and Class Members to safeguard their Private Information;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Defendant should have discovered the Data Breach sooner;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

151. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

152. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

153. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same network and unlawfully accessed in the same way.



1 The common issues arising from Defendant's conduct affecting Class Members set  
2 out above predominate over any individualized issues. Adjudication of these common  
3 issues in a single action has important and desirable advantages of judicial economy.

4 154. Superiority. A class action is superior to other available methods for the  
5 fair and efficient adjudication of the controversy. Class treatment of common  
6 questions of law and fact is superior to multiple individual actions or piecemeal  
7 litigation. Absent a class action, most Class Members would likely find that the cost  
8 of litigating their individual claims is prohibitively high and would therefore have no  
9 effective remedy. The prosecution of separate actions by individual Class Members  
10 would create a risk of inconsistent or varying adjudications with respect to individual  
11 Class Members, which would establish incompatible standards of conduct for  
12 Defendant. In contrast, to conduct this action as a class action presents far fewer  
13 management difficulties, conserves judicial resources and the parties' resources, and  
14 protects the rights of each Class Member.

15 155. Defendant has acted on grounds that apply generally to the Class as a  
16 whole, so that Class certification, injunctive relief, and corresponding declaratory  
17 relief are appropriate on a Class-wide basis.

18 156. Likewise, particular issues are appropriate for certification because such  
19 claims present only particular, common issues, the resolution of which would advance  
20 the disposition of this matter and the parties' interests therein. Such particular issues  
21 include, but are not limited to:

- 22 a. Whether Defendant failed to timely notify the public of the  
23 Data Breach;
- 24 b. Whether Defendant owed a legal duty to Plaintiff and the  
25 Class to exercise due care in collecting, storing, and  
26 safeguarding their Private Information;
- 27 c. Whether Defendant's security measures to protect its data  
28 systems were reasonable in light of best practices  
recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

157. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified by Defendant.

## **CLAIMS FOR RELIEF**

### **COUNT I**

#### **Negligence**

#### ***(On Behalf of Plaintiff and the Class)***

158. Plaintiff realleges and incorporates by reference allegations contained in the paragraphs 1 through 157, as though fully set forth herein.

159. By collecting and storing the Private Information of Plaintiff and Class Members, in its computer systems and networks, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

160. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed

1 herein, and to ensure that its systems and networks, and the personnel responsible for  
2 them, adequately protected the Private Information.

3 161. Plaintiff and Class Members are a well-defined, foreseeable, and  
4 probable group of consumers that Defendant was aware, or should have been aware,  
5 could be injured by inadequate data security measures.

6 162. Defendant's duty of care to use reasonable security measures arose as a  
7 result of the special relationship that existed between Defendant and consumers,  
8 which is recognized by laws and regulations including but not limited to the FTC Act  
9 and common law. Defendant was in a superior position to ensure that its systems were  
10 sufficient to protect against the foreseeable risk of harm to Plaintiff and Class  
11 Members from a data breach.

12 163. Defendant had a duty to employ reasonable security measures under  
13 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits  
14 "unfair ... practices in or affecting commerce," including, as interpreted and enforced  
15 by the FTC, the unfair practice of failing to use reasonable measures to protect  
16 confidential data.

17 164. Defendant's duty to use reasonable care in protecting confidential data  
18 arose not only as a result of the statutes and regulations described above, but also  
19 because Defendant is bound by industry standards to protect confidential Private  
20 Information.

21 165. Defendant breached its duties, and thus was negligent, by failing to use  
22 reasonable measures to protect Plaintiff's and Class Members' Private Information.  
23 The specific negligent acts and omissions committed by Defendant include, but are  
24 not limited to, the following:

- 25 a. Failing to adopt, implement, and maintain adequate
- 26 security measures to safeguard Plaintiff's and Class
- 27 Members' Private Information;
- 28

- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to ensure that its email systems had plans in place to maintain reasonable data security safeguards;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;
- f. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and
- g. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

166. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendant's possession.

167. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

168. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

169. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with

1 timely notice that their sensitive Private Information had been compromised.

2 170. Neither Plaintiff nor Class Members contributed to the Data Breach and  
3 subsequent misuse of their Private Information as described in this Complaint.

4 171. Plaintiff and Class Members are also entitled to injunctive relief  
5 requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring  
6 procedures; (ii) submit to future annual audits of those systems and monitoring  
7 procedures; and (iii) continue to provide adequate credit monitoring to all Class  
8 Members.

9 172. The injury and harm Plaintiff and Class Members suffered was the  
10 reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or  
11 should have known that it was failing to meet its duties, and that Defendant's breach  
12 would cause Plaintiff and Class Members to experience the foreseeable harms  
13 associated with the exposure of their Private Information.

14 173. As a direct and proximate result of Defendant's negligent conduct,  
15 Plaintiff and Class Members have suffered injury and are entitled to compensatory  
16 and consequential damages in an amount to be proven at trial.

## 17 COUNT II

### 18 **Breach of Implied Contract**

#### 19 ***(On Behalf of Plaintiff and the Class)***

20 174. Plaintiff realleges and incorporates by reference allegations contained in  
21 the paragraphs 1 through 157, as though fully set forth herein.

22 175. Defendant acquired and maintained the Private Information of Plaintiff  
23 and the Class that they received either directly or indirectly.

24 176. When Plaintiff and Class Members paid money and provided their  
25 Private Information to loanDepot, either directly or indirectly, in exchange for goods  
26 or services, they entered into implied contracts with loanDepot, their business  
27 associates, revenue service providers, and other service providers, including  
28 Defendant.

1 177. Plaintiff and Class Members entered into implied contracts with  
2 Defendant under which Defendant agreed to safeguard and protect their Private  
3 Information and to timely and accurately notify Plaintiff and Class Members that their  
4 information had been breached and compromised.

5 178. Plaintiff and the Class were required to entrust their Private Information  
6 to Defendant as part of the process of obtaining services provided by Defendant.  
7 Plaintiff and Class Members paid money, or money was paid on their behalf, to  
8 Defendant in exchange for services.

9 179. Defendant loanDepot solicited, offered, and invited Class Members to  
10 provide their Private Information as part of Defendant's regular business practices.  
11 Plaintiff and Class Members accepted Defendant's offers and provided their Private  
12 Information to Defendant.

13 180. Defendant accepted possession of Plaintiff's and Class Members'  
14 Private Information for the purpose of providing services to Plaintiff and Class  
15 Members.

16 181. In accepting such information and payment for services, Defendant  
17 entered into implied contracts with Plaintiff and Class Members whereby Defendant  
18 became obligated to reasonably safeguard Plaintiff's and Class Members' Private  
19 Information.

20 182. Alternatively, Plaintiff and Class Members were the intended  
21 beneficiaries of data protection agreements entered into between Defendant and its  
22 business associates.

23 183. In delivering, directly or indirectly, their Private Information to  
24 Defendant and paying for financial services, Plaintiff and Class Members intended  
25 and understood that Defendant would adequately safeguard the data as part of that  
26 service.

27 184. The implied promise of confidentiality includes consideration beyond  
28 those pre-existing general duties owed under state or federal regulations. The

1 additional consideration included implied promises to take adequate steps to comply  
2 with specific industry data security standards and FTC guidelines on data security.

3 185. The implied promises include but are not limited to: (1) taking steps to  
4 ensure that any agents who are granted access to Private Information also protect the  
5 confidentiality of that data; (2) taking steps to ensure that the information that is  
6 placed in the control of their agents is restricted and limited to achieve an authorized  
7 purpose; (3) restricting access to qualified and trained agents; (4) designing and  
8 implementing appropriate retention policies to protect the information against  
9 criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor  
10 authentication for access; and (7) other steps to protect against foreseeable data  
11 breaches.

12 186. Plaintiff and Class Members would not have entrusted their Private  
13 Information to Defendant in the absence of such an implied contract.

14 187. Had Defendant disclosed to Plaintiff and Class Members that they did  
15 not have adequate computer systems and security practices to secure sensitive data,  
16 Plaintiff and Class Members would not have provided their Private Information to  
17 Defendant.

18 188. Defendant recognized that Plaintiff's and Class Members' Private  
19 Information is highly sensitive and must be protected, and that this protection was of  
20 material importance as part of the bargain to Plaintiff and Class Members.

21 189. Plaintiff and Class Members fully performed their obligations under the  
22 implied contracts with Defendant.

23 190. Defendant breached the implied contracts with Plaintiff and Class  
24 Members by failing to take reasonable measures to safeguard their Private  
25 Information as described herein.

26 191. As a direct and proximate result of Defendant's conduct, Plaintiff and  
27 the other Class Members suffered and will continue to suffer damages in an amount  
28 to be proven at trial.



**COUNT III****Unjust Enrichment*****(On Behalf of Plaintiff and the Class)***

192. Plaintiff realleges and incorporates by reference allegations contained in the paragraphs 1 through 157, as though fully set forth herein.

193. This count is pleaded in the alternative to breach of contract.

194. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from money it makes based upon protecting Plaintiff's and Class Members' Private Information.

195. There is a direct nexus between money paid to Defendant and the requirement that Defendant keeps Plaintiff's and Class Members' Private Information confidential and protected.

196. Plaintiff and Class Members paid Defendant a certain sum of money, which was used to fund data security via contracts with Defendant.

197. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

198. Protecting the Private Information of Plaintiff and Class Members is integral to Defendant's businesses. Without their data, loanDepot would be unable to provide the financial services comprising loanDepot's core business.

199. Plaintiff's and Class Members' data and Private Information has monetary value.

200. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from entities that contracted with Defendant, and from which Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by

1 supplying Private Information, which has value, from which value Defendant derives  
2 its business value, and which should have been protected with adequate data security.

3 201. Defendant knew that Plaintiff and Class Members conferred a benefit  
4 which Defendant accepted. Defendant profited from these transactions and used the  
5 Private Information of Plaintiff and Class Members for business purposes.

6 202. Defendant enriched itself by saving the costs it reasonably should have  
7 expended on data security measures to secure Plaintiff's and Class Members' Private  
8 Information. Instead of providing a reasonable level of security that would have  
9 prevented the Data Breach, Defendant instead calculated to avoid its data security  
10 obligations at the expense of Plaintiff and Class Members by utilizing cheaper,  
11 ineffective security measures. Plaintiff and Class Members, on the other hand,  
12 suffered as a direct and proximate result of Defendant's failures to provide the  
13 requisite security.

14 203. Under the principles of equity and good conscience, Defendant should  
15 not be permitted to retain the money belonging to Plaintiff and Class Members,  
16 because Defendant failed to implement appropriate data management and security  
17 measures that are mandated by industry standards.

18 204. Defendant acquired the monetary benefit and Private Information  
19 through inequitable means in that it failed to disclose the inadequate security practices  
20 previously alleged.

21 205. If Plaintiff and Class Members knew that Defendant had not secured  
22 their Private Information, they would not have agreed to provide their Private  
23 Information to Defendant.

24 206. Plaintiff and Class Members have no adequate remedy at law.

25 207. As a direct and proximate result of Defendant's conduct, Plaintiff and  
26 Class Members have suffered and will suffer injury, including but not limited to: (i)  
27 actual identity theft; (ii) the loss of the opportunity to control how their Private  
28 Information is used; (iii) the compromise, publication, and/or theft of their Private

Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; (vii) loss of privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

208. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

209. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

#### **COUNT IV**

##### **Bailment**

##### ***(On Behalf of Plaintiff and the Class)***

210. Plaintiff realleges and incorporates by reference allegations contained in the paragraphs 1 through 157, as though fully set forth herein.

211. Plaintiff and Class Members provided Private Information to Defendant—either directly or indirectly—which Defendant was under a duty to keep private and confidential.

212. Plaintiff's and Class Members' Private Information is personal property and was conveyed to Defendant for the certain purpose of keeping the information private and confidential.

213. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

214. Once Defendant accepted Plaintiff's and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendant.

215. Defendant did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

216. Defendant's failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

217. As a result of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

## **COUNT V**

### **Breach of Fiduciary Duty**

#### ***(On Behalf of Plaintiff and the Class)***

218. Plaintiff realleges and incorporates by reference allegations contained in the paragraphs 1 through 157, as though fully set forth herein.

1           219. In light of the special relationship between Defendant and Plaintiff and  
2 Class Members, Defendant became a fiduciary by undertaking a guardianship of the  
3 Private Information to act primarily for Plaintiff and Class Members, (1) for the  
4 safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely  
5 notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to  
6 maintain complete and accurate records of what information (and where) Defendant  
7 does store.

8           220. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class  
9 Members upon matters within the scope of their relationship with consumers, in  
10 particular, to keep secure their Private Information.

11           221. Defendant breached its fiduciary duty to Plaintiff and Class Members by  
12 failing to encrypt and otherwise protect the integrity of the systems containing  
13 Plaintiff's and Class Members' Private Information.

14           222. Defendant breached its fiduciary duty to Plaintiff and Class Members by  
15 otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

16           223. As a direct and proximate result of Defendant's breach of its fiduciary  
17 duties, Plaintiff and Class Members have suffered and will suffer injury, including but  
18 not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of  
19 their Private Information; (iii) out-of-pocket expenses associated with the prevention,  
20 detection, and recovery from identity theft and/or unauthorized use of their Private  
21 Information; (iv) lost opportunity costs associated with effort expended and the loss  
22 of productivity addressing and attempting to mitigate the actual and future  
23 consequences of the Data Breach, including but not limited to efforts spent  
24 researching how to prevent, detect, contest, and recover from identity theft; (v) the  
25 continued risk to their Private Information, which remains in Defendant's possession  
26 and is subject to further unauthorized disclosures so long as Defendant fails to  
27 undertake appropriate and adequate measures to protect the Private Information in its  
28 continued possession; (vi) future costs in terms of time, effort, and money that will be

1 expended as result of the Data Breach for the remainder of the lives of Plaintiff and  
 2 Class Members; and (vii) the diminished value of Defendant's services they received.

3 224. As a direct and proximate result of Defendant's breach of its fiduciary  
 4 duties, Plaintiff and Class Members have suffered and will continue to suffer other  
 5 forms of injury and/or harm, and other economic and non-economic losses.

### 6 **PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiff prays for judgment as follows:

8 a) For an Order certifying this action as a Class Action and appointing  
 9 Plaintiff as Class Representative and his counsel as Class Counsel;

10 b) For equitable relief enjoining Defendant from engaging in the wrongful  
 11 conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's  
 12 and Class Members' Private Information, and from refusing to issue prompt, complete  
 13 and accurate disclosures to Plaintiff and Class Members;

14 c) For equitable relief compelling Defendant to utilize appropriate methods  
 15 and policies with respect to consumer data collection, storage, and safety, and to  
 16 disclose with specificity the type of Private Information compromised during the Data  
 17 Breach;

18 d) For equitable relief requiring restitution and disgorgement of the  
 19 revenues wrongfully retained as a result of Defendant's wrongful conduct;

20 e) Ordering Defendant to pay for not less than five years of credit  
 21 monitoring services for Plaintiff and the Class;

22 f) For an award of actual damages, compensatory damages, statutory  
 23 damages, nominal damages, and/or statutory penalties, in an amount to be determined,  
 24 as allowable by law;

25 g) For an award of punitive damages, as allowable by law;

26 h) Pre- and post-judgment interest on any amounts awarded; and,

27 i) Such other and further relief as this court may deem just and proper.

PEARSON WARSHAW, LLP  
15165 VENTURA BOULEVARD, SUITE 400  
SHERMAN OAKS, CALIFORNIA 91403

**DEMAND FOR JURY TRIAL**

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

DATED: February 7, 2024

**PEARSON WARSHAW, LLP**

By: /s/ Daniel L. Warshaw  
DANIEL L. WARSHAW

DANIEL L. WARSHAW (Bar No. 185365)  
dwarshaw@pwwfirm.com  
**PEARSON WARSHAW, LLP**  
15165 Ventura Boulevard, Suite 400  
Sherman Oaks, California 91403  
Telephone: (818) 788-8300  
Facsimile: (818) 788-8104

STEVEN M. NATHAN, (Bar No. 153250)  
snathan@hausfeld.com  
**HAUSFELD LLP**  
33 Whitehall Street  
Fourteenth Floor  
New York, NY 10004  
Telephone: (646) 357-1100  
Facsimile: (212) 202-4322

JAMES J. PIZZIRUSSO\*  
jpizzirusso@hausfeld.com  
**HAUSFELD LLP**  
888 16th Street, N.W., Suite 300  
Washington, D.C. 20006  
Telephone: (202) 540-7200  
Facsimile: (202) 540-7201

*Counsel for Plaintiff and the Proposed Class*

*\*Pro Hac Vice Forthcoming*



# EXHIBIT A



# loanDepot is experiencing a cyber incident.

## **January 26, 2024 – 12:00pm ET**

For our loan servicing customers, late fees for January payments will not be assessed until after January 31.

## **January 22, 2024 – 9:00am ET**

loanDepot today provided an [update](https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx) (<https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx>) on its cyber incident.

Our Customer Care team is available to answer customer questions related to this announcement at 888-337-6888. Select option 4 and then enter extension 6789. We will soon have a dedicated toll-free number that customers can call to ask questions about this event, which we will post to this page as soon as it is available.

## **January 19, 2024 – 5:00pm ET**

Our [Servicing customer portal](https://servicing.loandepot.com/) (<https://servicing.loandepot.com/>) and mobile app are now fully operational.

## **January 18, 2024 – 3:30pm ET**

mellohome's [website](https://www.mellohome.com/) (<https://www.mellohome.com/>) is back online.

## **January 18, 2024 – 2:30pm ET**

The [MyloanDepot customer portal](https://apply.loandepot.com/user/login) (<https://apply.loandepot.com/user/login>) for online loan applications and status tracking is back online.

## **January 18, 2024 – 12:00pm ET**

Our [HELOC customer portal](https://myheloc.loandepot.com/) (<https://myheloc.loandepot.com/>) is back online.

**January 18, 2024 – 10:00am ET**

loanDepot's Servicing customer portal (<https://servicing.loandepot.com>) is back online (with some limits to functionality). We will continue to post operational updates on this page as we return to normal business operations.

**January 16, 2024 – 3:30pm ET**

For our loan servicing customers, year-end statements (IRS Form 1098) were mailed January 16 to the mailing address on file and will be posted to our Servicing customer portal (<https://servicing.loandepot.com>) as soon as our systems are back online.

**January 14, 2024 – 9:30am ET**

Our customers continue to be our top priority, and we are working diligently to restore normal business operations as quickly as possible.

For our loan servicing customers, recurring automatic payments continue to process as expected, but there may be a temporary delay in viewing the posted payment in your payment history. Customers seeking to make a payment may do so through our loan servicing contact center at 866-258-6572 from 7 am CT to 7 pm CT Monday through Friday, and 8 am to 5 pm CT on Saturday. They may also mail their payment with their loan number to the address on their statement. Late fees will not be assessed until after January 25. We apologize for any inconvenience.

**January 8, 2024 – 6:00am ET**

loanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these matters as soon as possible.

---

***Operational updates will be posted to this page.***





(/)

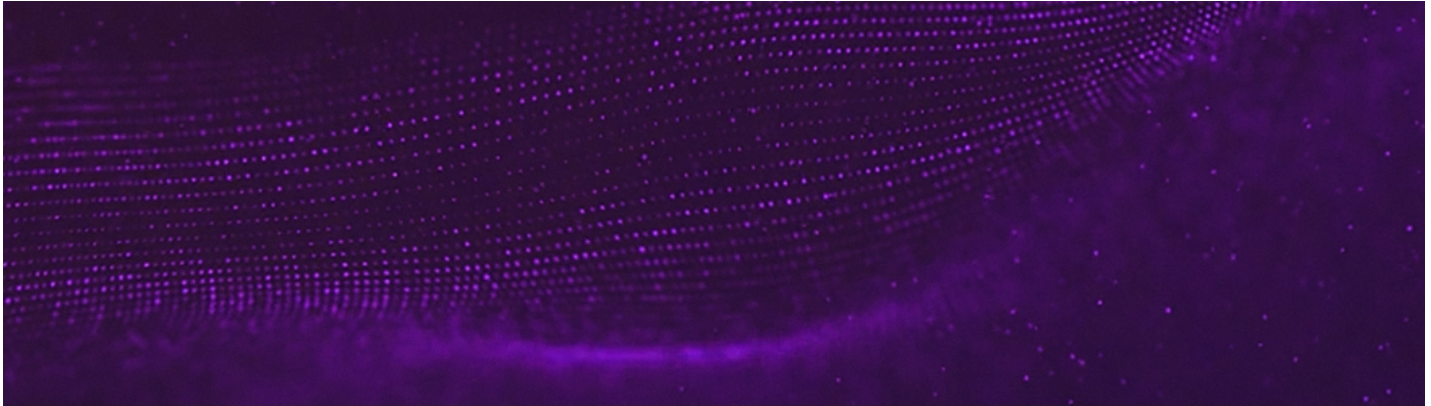
© 2009–2024 loanDepot, Inc. All rights reserved.

Privacy Policy (<https://www.loandepot.com/privacypolicy>)



OVERVIEW NEWS RELEASES OUR HISTORY SPOKESPEOPLE MULTIMEDIA 

MEDIA RESOURCES 



**VIEW ALL NEWS >**

# loanDepot Provides Update on Cyber Incident

01/22/2024

IRVINE, Calif.--(BUSINESS WIRE)-- loanDepot, Inc. ("LDI" or "Company") (NYSE: LDI), a leading provider of home lending solutions, today provided an update on the cyber incident it disclosed on January 8, 2024.

The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyloanDepot and Servicing customer portals.

Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.

"Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers," said loanDepot CEO Frank Martell. "The entire loanDepot team has worked tirelessly throughout this incident to support our customers, our partners and each other. I am pleased by our progress in quickly bringing our systems back online and restoring normal business operations."

"Our customers are at the center of everything we do," said Jeff Walsh, President of LDI Mortgage. "I'm really proud of our team, and we're glad to be back to doing what we do best: enabling our customers across the country to achieve their financial goals and dreams of homeownership."

The Company is committed to keeping its customers, partners and employees informed and will provide any additional operational updates on our microsite at [loandepot.cyberincidentupdate.com](https://loandepot.cyberincidentupdate.com).

## About loanDepot

loanDepot (NYSE: LDI; NMLS # 174457) is an equal housing lender and digital commerce company committed to serving its customers throughout the homeownership journey. Since its launch in 2010, loanDepot has revolutionized the mortgage industry with a digital-first approach that makes it easier, faster and less stressful to purchase or refinance a home. Today, as one of the nation's largest non-bank retail mortgage lenders, loanDepot enables customers to achieve the American dream of homeownership through a broad suite of lending and real estate services that simplify one of life's most complex transactions.



[OVERVIEW](#) [NEWS RELEASES](#) [OUR HISTORY](#) [SPOKESPEOPLE](#)

Jonathan Fine, VP, Public Relations  
(781) 248-3963, [jfine@loandepot.com](mailto:jfine@loandepot.com)

Source: loanDepot, Inc.


[VIEW ALL NEWS >](#)

## Follow Us



## Media Contact

Jonathan Fine  
VP, Public Relations

 (949) 936-0257

 [JFINE@LOANDEPOT.COM](mailto:jfine@loandepot.com)

## Sign Up for loanDepot, Inc. News Alerts

[SIGN UP](#)

[Unsubscribe](#)



[Accessibility statement](#) | [Privacy and Security](#) | [Terms of Use](#) | [Cookies Policy](#) | [Site Map](#)

(C) 2009-2023 loanDepot, Inc. All rights reserved.

Powered By Q4 Inc. 5.115.1.9